GENERAL OVERVIEW OF STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

[*45 CFR Part 160 and Subparts A and E of Part 164*]

The following overview provides answers to general questions regarding the *Standards for Privacy of Individually Identifiable Health Information* (the Privacy Rule), promulgated by the Department of Health and Human Services (HHS).

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, included "Administrative Simplification" provisions that required HHS to adopt national standards for electronic health care transactions. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

In response to the HIPAA mandate, HHS published a final regulation in the form of the Privacy Rule in December 2000, which became effective on April 14, 2001. This Rule set national standards for the protection of health information, as applied to the three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct certain health care transactions electronically. By the compliance date of April 14, 2003 (April 14, 2004, for small health plans), covered entities must implement standards to protect and guard against the misuse of individually identifiable health information. Failure to timely implement these standards may, under certain circumstances, trigger the imposition of civil or criminal penalties.

Secretary Tommy Thompson called for an additional opportunity for public comment on the Privacy Rule to ensure that the Privacy Rule achieves its intended purpose without adversely affecting the quality of, or creating new barriers to, patient care. After careful consideration of these comments, in March 2002 HHS published proposed modifications to the Rule, to improve workability and avoid unintended consequences that could have impeded patient access to delivery of quality health care. Following another round of public comment, in August 2002, the Department adopted as a final Rule the modifications necessary to ensure that the Privacy Rule worked as intended.

The Privacy Rule establishes, for the first time, a foundation of Federal protections for the privacy of protected health information. The Rule does not replace Federal, State, or other law that grants individuals even greater privacy protections, and covered entities are free to retain or adopt more protective policies or practices.

GENERAL OVERVIEW

Frequently Asked Questions

Q: What does the HIPAA Privacy Rule do?

A: Most health plans and health care providers that are covered by the new Rule must comply with the new requirements by April 14, 2003.

The HIPAA Privacy Rule for the first time creates national standards to protect individuals' medical records and other personal health information.

- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.
- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights
- And it strikes a balance when public responsibility supports disclosure of some forms of data – for example, to protect public health.

For patients – it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used.

- It enables patients to find out how their information may be used, and about certain disclosures of their information that have been made.
- It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure.
- It generally gives patients the right to examine and obtain a copy of their own health records and request corrections.
- It empowers individuals to control certain uses and disclosures of their health information.

Q: Why is the HIPAA Privacy Rule needed?

A: In enacting HIPAA, Congress mandated the establishment of Federal standards for the privacy of individually identifiable health information. When it comes to personal information that moves across hospitals, doctors' offices, insurers or third party payers, and State lines, our country has relied on a patchwork of Federal and State laws. Under the patchwork of laws existing prior to adoption of HIPAA and the Privacy Rule, personal health information could be distributed—without either notice or authorization—for reasons that had nothing to do with a patient's medical treatment or health care reimbursement. For example, unless otherwise forbidden by State or local law, without the Privacy Rule patient information held by a health plan could, without the patient's permission, be passed on to a lender who could then deny the patient's application for a home mortgage or a credit card, or to an employer who could use it in personnel decisions. The Privacy Rule establishes a Federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections will continue to apply over and above the new Federal privacy standards.

Health care providers have a strong tradition of safeguarding private health information. However, in today's world, the old system of paper records in locked filing cabinets is not enough. With information broadly held and transmitted electronically, the Rule provides clear standards for the protection of personal health information.

Q: Generally, what does the HIPAA Privacy Rule require the average provider or health plan to do?

A: For the average health care provider or health plan, the Privacy Rule requires activities, such as:

- Notifying patients about their privacy rights and how their information can be used.
- Adopting and implementing privacy procedures for its practice, hospital, or plan.
- Training employees so that they understand the privacy procedures.
- Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

Responsible health care providers and businesses already take many of the kinds of steps

required by the Rule to protect patients' privacy. Covered entities of all types and sizes are required to comply with the Privacy Rule. To ease the burden of complying with the new requirements, the Privacy Rule gives needed flexibility for providers and plans to create their own privacy procedures, tailored to fit their size and needs. The scalability of the Rule provides a more efficient and appropriate means of safeguarding protected health information than would any single standard. For example,

- The privacy official at a small physician practice may be the office manager, who will have other non-privacy related duties; the privacy official at a large health plan may be a full-time position, and may have the regular support and advice of a privacy staff or board.

- The training requirement may be satisfied by a small physician practice's providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed the policies; whereas a large health plan may provide training through live instruction, video presentations, or interactive software programs.

- The policies and procedures of small providers may be more limited under the Rule than those of a large hospital or health plan, based on the volume of health information maintained and the number of interactions with those within and outside of the health care system.

Q: Who must comply with these new HIPAA privacy standards?

A: As required by Congress in HIPAA, the Privacy Rule covers:

- Health plans

- Health care clearinghouses

- Health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards have been adopted by the Secretary under HIPAA, such as electronic billing and fund transfers.

These entities (collectively called "covered entities") are bound by the new privacy standards even if they contract with others (called "business associates") to perform some of their essential functions. The law does not give the Department of Health and Human Services (HHS) the authority to regulate other types of private businesses or public agencies through this regulation. For example, HHS does not have the authority to

regulate employers, life insurance companies, or public agencies that deliver social security or welfare benefits. See the fact sheet and frequently asked questions on this web site about the standards on "Business Associates" for a more detailed discussion of the covered entities' responsibilities when they engage others to perform essential functions or services for them.

Q: When will covered entities have to meet these HIPAA privacy standards?

A: As Congress required in HIPAA, most covered entities have until April 14, 2003 to come into compliance with these standards, as modified by the August, 2002 final Rule. Small health plans will have an additional year – until April 14, 2004 – to come into compliance.

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is providing assistance to help covered entities prepare to comply with the Rule. For example, OCR maintains a web site with helpful information, such as the Guidance, Frequently Asked Questions, sample "business associate" contract provisions, significant reference documents, and other technical assistance information for consumers and the health care industry, at http://www.hhs.gov/ocr/hipaa/.

Q: What were the major modifications to the HIPAA Privacy Rule that the Department of Health and Human Services (HHS) adopted in August 2002?

A: Based on the information received through public comments, testimony at public hearings, meetings at the request of industry and other stakeholders, as well as other communications, HHS identified a number of areas in which the Privacy Rule, as issued in December 2000, would have had potential unintended effects on health care quality or access. As a result, HHS proposed modifications that would maintain strong protections for the privacy of individually identifiable health information, address the unintended negative effects of the Privacy Rule on health care quality or access to health care, and relieve unintended administrative burdens created by the Privacy Rule.

Final modifications to the Rule were adopted on August 14, 2002. Among other things, the modifications addressed the following aspects of the Privacy Rule:

- Uses and disclosures for treatment, payment and health care operations, including eliminating the requirement for the individual's consent for these activities;
- The notice of privacy practices that covered entities must provide to patients;
- Uses and disclosures for marketing purposes;

- Minimum necessary uses and disclosures;
- Parents as the personal representatives of unemancipated minors;
- Uses and disclosures for research purposes; and
- Transition provisions, including business associate contracts.

In addition to these key areas, the modifications included changes to certain other provisions where necessary to clarify the Privacy Rule, and a list of technical corrections intended as editorial or typographical corrections to the Privacy Rule.

For more information about the final modifications to the Privacy Rule, see the Fact Sheet entitled, *Modifications to the Standards for Privacy of Individually Identifiable Health Information – Final Rule*. This Fact Sheet can be found at http://www.hhs.gov/news/press/2002pres/20020809.html.

Q: Why was the consent requirement eliminated from the HIPAA Privacy Rule, and how will it affect individuals' privacy protections?

A: The consent requirement created the unintended effect of preventing health care providers from providing timely, quality health care to individuals in a variety of circumstances. The most troubling and pervasive problem was that health care providers would not have been able to use or disclose protected health information for treatment, payment, or health care operations purposes prior to the initial face-to-face encounter with the patient, which is routinely done to provide timely access to quality health care. The following are some examples of how the consent requirement would have posed barriers to health care:

- Pharmacists would not have been able to fill a prescription, search for potential drug interactions, determine eligibility, or verify coverage before the individual arrived at the pharmacy to pick up the prescription if the individual had not already provided consent under the Privacy Rule.
- Hospitals would not have been able to use information from a referring physician to schedule and prepare for procedures before the individual presented at the hospital for such procedure, or the patient would have had to make a special trip to the hospital to sign the consent form.
- Providers who do not provide treatment in person (such as a provider prescribing over the telephone) may have been unable to provide care because they would

have had difficulty obtaining prior written consent to use protected health information at the first service delivery.

- Emergency medical providers were concerned that, even if a situation was urgent, they would have had to try to obtain consent to comply with the Privacy Rule, even if that would be inconsistent with the appropriate practice of emergency medicine.

- Emergency medical providers were also concerned that the requirement that they attempt to obtain consent as soon as reasonably practicable after an emergency would have required significant efforts and administrative burden which might have been viewed as harassing by patients, because these providers typically do not have ongoing relationships with individuals.

To eliminate such barriers to health care, mandatory consent was replaced with the voluntary consent provision that permits health care providers to obtain consent for treatment, payment and healthcare operations, at their option, and enables them to obtain consent in a manner that does not disrupt needed treatment. Although consent is no longer mandatory, the Rule still affords individuals the opportunity to engage in important discussions regarding the use and disclosure of their health information through the strengthened notice requirement, while allowing activities that are essential to quality health care to occur unimpeded. These modifications will ensure that the Rule protects patient privacy as intended without harming consumers' access to care or the quality of that care. Further, the individual's right to request restrictions on the use or disclosure of his or her protected health information is retained in the Rule as modified.

Q: Did the final modifications to the HIPAA Privacy Rule alter the compliance date(s) for covered entities?

A: No. The compliance dates for the Privacy Rule, as modified, remain April 14, 2003, for most health plans, covered health care providers, and health care clearinghouses, and April 14, 2004, for small health plans. Under HIPAA, compliance with a modification to an existing standard or implementation specification is required by a date set by the Secretary, but not earlier than 180 days from the adoption of the modification. By publishing the modifications to the Privacy Rule in August 2002, the original compliance date of April 2003 is maintained for the entire Rule, as modified.

Q: Will the Department of Health and Human Services (HHS) make future changes to the HIPAA Privacy Rule and, if so, how will these changes be made?

A: Under HIPAA, HHS has the authority to modify the privacy standards as the Secretary

may deem appropriate. However, a standard can be modified only once in a 12-month period.

As a general rule, future modifications to the Privacy Rule must be made in accordance with the Administrative Procedure Act (APA). HHS will comply with the APA by publishing proposed rule changes, if any, in the *Federal Register* through a Notice of Proposed Rulemaking and will invite comment from the public. After reviewing and addressing those comments, HHS will issue a modified final rule.